— AUS（アルテミス・ユーザ・サポート）便り 2017/10/02号 —
https://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

## ●悪意のあるプログラムが実行される「DLL読み込みの脆弱性」が急増、IPAが対策呼びかけ

http://itpro.nikkeibp.co.jp/atcl/news/17/092802357/
https://www.ipa.go.jp/security/ciadr/vul/20170928_dll.html

### このニュースをザックリ言うと・・・

- 9月28日（日本時間）、情報処理推進機構（IPA）より、Windows上のアプリにおいて「DLL読み込みの脆弱性」が多く報告されていることについて、注意が呼び掛けられています。

- この脆弱性は、アプリの実行時、「DLL（動的ライブラリ）がアプリファイルと同じフォルダに置かれていた場合にそれを読み込む」という挙動に起因するもので、例えば、「ダウンロードフォルダに何らかのアプリのインストーラーと不正なDLLが同時に保存されている」状態でインストーラーを実行することにより、悪意のあるコードが実行される可能性があるとされています。

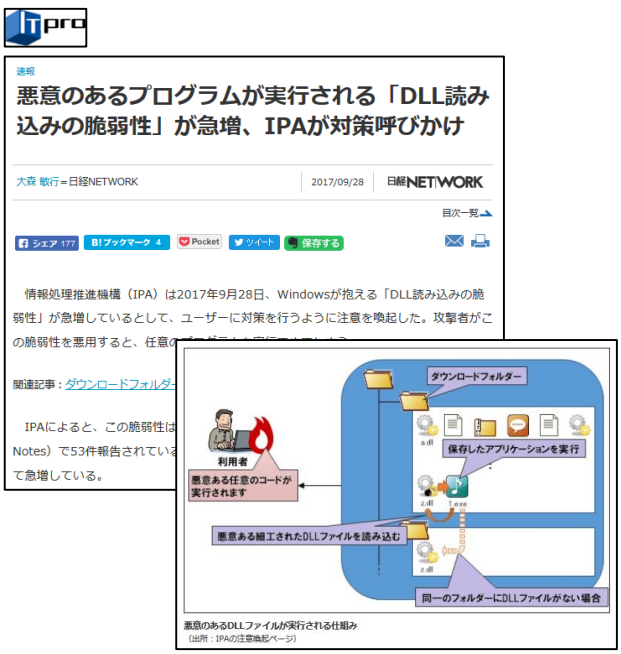
- IPA等が運営する脆弱性情報サイト「JVN」では、4月から8月末までの間に53件の脆弱性が報告されたとしています。

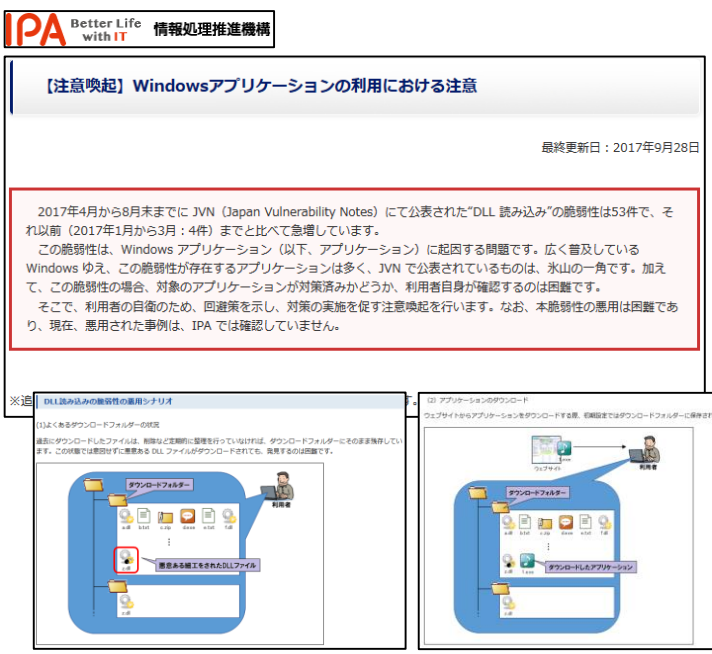
### AUS便りからの所感等

- 当該脆弱性およびそれを悪用する「DLLインジェクション攻撃」については、当AUS便りの2017/06/05号でも紹介しており、以降、対策がとられたものも多いとみられますが、如何せん多くのソフトウェアで問題が存在していたことから、今回の再度の注意喚起となったとみられます。

- Webブラウザでのデフォルトの設定では、ダウンロードしたファイルがすべて特定のダウンロードフォルダに保存されるようになっており、通常はそのままインストーラーなどを実行するという行動をとることが考えられるため、その分だけ攻撃者にとっては準備をし易い状況にあると言えます。

- アンチウイルス・UTM等で「ダウンロードフォルダ上に不正なDLLを展開する」等の挙動を阻止してくれるかは未知数ですが、IPAが回避策として推奨している「ダウンロードフォルダ自体ではなく新規に別のフォルダを作成して保存する」「(アプリがある)フォルダ内に正規のファイル以外が保存されていないか確認する」を可能な限りとるべきでしょう。


速報
悪意のあるプログラムが実行される「DLL読み込みの脆弱性」が急増、IPAが対策呼びかけ
大森 敬行＝日経NETWORK　2017/09/28　日経NETWORK
目次一覧
シェア 177　Bブックマーク 4　Pocket　ツイート　保存する
情報処理推進機構（IPA）は2017年9月28日、Windowsが抱える「DLL読み込みの脆弱性」が急増しているとして、ユーザーに対策を行うように注意を喚起した。攻撃者がこの脆弱性を悪用すると、任意の
関連記事：ダウンロードフォルダ
IPAによると、この脆弱性は
Notes）で53件報告されている
て急増している。
ダウンロードフォルダー
保存したアプリケーションを実行
利用者
悪意ある任意のコードが実行されます
悪意ある細工されたDLLファイルを読み込む
同一のフォルダーにDLLファイルがない場合
悪意のあるDLLファイルが実行される仕組み
（出所：IPAの注意喚起ページ）


IPA Better Life with IT 情報処理推進機構
【注意喚起】Windowsアプリケーションの利用における注意
最終更新日：2017年9月28日
2017年4月から8月末までに JVN（Japan Vulnerability Notes）にて公表された"DLL 読み込み"の脆弱性は53件で、それ以前（2017年1月から3月：4件）までと比べて急増しています。
この脆弱性は、Windows アプリケーション（以下、アプリケーション）に起因する問題です。広く普及している Windows ゆえ、この脆弱性が存在するアプリケーションは多く、JVN で公表されているものは、氷山の一角です。加えて、この脆弱性の場合、対象のアプリケーションが対策済みかどうか、利用者自身が確認するのは困難です。
そこで、利用者の自衛のため、回避策を示し、対策の実施を促す注意喚起を行います。なお、本脆弱性の悪用は困難であり、現在、悪用された事例は、IPA では確認していません。
※追
DLL読み込みの脆弱性の悪用シナリオ
(1)よくあるダウンロードフォルダーの状況
ダウンロードフォルダー
利用者
悪意ある細工されたDLLファイル
(2) アプリケーションのダウンロード
ウェブサイトからアプリケーションをダウンロードする際、初期設定ではダウンロードフォルダーに保存されます。
ウェブサイト
利用者
ダウンロードフォルダー
ダウンロードしたアプリケーション

# ●東京は世界屈指の「ボットスポット」…シマンテック調査

http://internet.watch.impress.co.jp/docs/news/1083591.html

## このニュースをザックリ言うと・・・

- 9月28日（日本時間）、大手セキュリティベンダーのシマンテック社より、ボットの日本国内における分布状況を把握できるウェブサイト「ボットスポット」が公開されました。

- 公開に伴う発表によれば、2016年における世界でのボット感染状況は2015年に比べ670万台増加しており、ボットネットが駆除されるまでの平均寿命も8日間から51日間へと伸びているとのことです。

- 日本でのボット分布数は全体の0.56%で、世界36位とされていますが、都道府県別での分布では東京都が最も多い60.92%で、UAE・アイルランド・オーストラリアといった国単位でのボットスポットの総数を上回るほどとの結果が出ています。

## AUS便りからの所感等

- ボットネットは既にPCのみをターゲットとするものではなくなっており、昨年は50万台ものIoT機器に感染した「Mirai」、つい最近でもAndroidの複数のアプリからスマートフォン等に感染した「WireX」等が挙げられます。

- こと近年では、通信量制限等があるモバイル回線を経由してDDoS攻撃が行われることにより、無料通信・高速通信分を早々に使い尽され、ユーザが正常な通信を行えなくなる等の損害を被る可能性が高くなっています。

- あらゆるデバイスにおいて、ボットに感染しないための入口対策と、感染後に外部の司令サーバへ接続されないための出口対策との両方を確実にとれるよう、アンチウイルスやUTM等を活用した防御態勢をとることが肝要です。

INTERNET Watch

**東京は世界屈指の"ボットスポット"～シマンテック調査**

岩崎 宰守　2017年9月29日 16:12


シマンテック株式会社は、ボットの日本国内における分布状況を把握できるウェブサイト「ボットスポット」を公開した。東京は国内のボット感染源の6割超が集中しているという。2016年のデータを元に4月に発行した「インターネットセキュリティ脅威レポート」に基づくもの。

# ●2種類のランサムウェアによる新たなスパムキャンペーン…2度感染する（身代金を2度払う）恐れも

https://japan.cnet.com/article/35107474/

## このニュースをザックリ言うと・・・

- 9月18日（現地時間）、大手セキュリティベンダーのトレンドマイクロ社より、スパムメールによってPCに2種類のランサムウェアを感染させようとする攻撃が確認されたとして、同社ブログにて注意喚起が出されています。

- 記事によれば、攻撃は請求書に偽装したメールで行われ、添付ファイルを開いた際にダウンロードされるランサムウェアとして、2016年に登場した「Locky」と、今年6月に登場した「FakeGlobe」とが数時間おきに差し替えられて利用されるとのことです。

- 同社の研究者は「LockyとFakeGlobeが交互にプッシュされているため、ファイルが最初とは違うランサムウェアで暗号化されるかもしれない」「被害者は身代金を2度払うか、最悪の場合、データを完全に失ってしまうことがある」と述べています。

## AUS便りからの所感等

- アンチウイルスやUTMがあるマルウェアに対応していたとして、別のマルウェアにも決して感染しないという保証はありませんが、不十分な防御であれば、このように複数のマルウェアに感染してしまうケースは決して珍しいことではありません。

- ランサムウェアに「絶対に感染しないこと」のみを意識するのではなく、「万が一に感染してしまったとき」を想定し、確実にデータ復旧が行えるような形でのバックアップの実施等の回避策をとっておくこともまた重要です。

cnet Japan

ランサムウェア

**2種類のランサムウェアによる新たなスパムキャンペーン--2度感染する恐れも**

Danny Palmer （ZDNet.com） 翻訳校正： 編集部　2017年09月20日 12時19分

ランサムウェアに感染するだけでも不運だが、新たに登場したサイバー攻撃の被害者は、ファイルを復号するための身代金を1度ならず、2度までも払わねばならない憂き目に遭う可能性があるという。

ランサムウェアを拡散するために、スパムメールを送りつけるのは何も目新しいことではない。しかし9月に検出された攻撃は、この常套手段にひねりを加えて、ランサムウェアのペイロードを順番に変えるという手法をとっている。

この攻撃は、再浮上した「Locky」と、6月に初めて登場した「FakeGlobe」の2つのランサムウェアを配布する。ペイロードを交換できるように設計されているため、スパムメールが最初にLockyを送りつけ、次にFakeGlobeを届ける可能性があるという。